**UNITED STATES DISTRICT COURT FOR THE MIDDLE DISTRICT OF TENNESSEE**

| | |
|---|---|
| Paula S. Gordy LISW, LLC, individually and on behalf of all others similarly situated,<br><br>Plaintiff(s),<br><br>v.<br><br>CHANGE HEALTHCARE INC.,<br><br>Defendant. | CASE NO.:<br><br>**CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

## CLASS ACTION COMPLAINT

Plaintiff Paula S. Gordy LISW, LLC ("Plaintiff"), by and through the undersigned counsel, brings this class action complaint against Defendant Change Healthcare Inc. ("Defendant" or "Change"), on behalf of itself and all others similarly situated. Plaintiff makes the following allegations based upon personal knowledge as to its own actions and upon information and belief as to all other matters:

## NATURE OF THE ACTION

1. "An urgent care chain in Ohio may be forced to stop paying rent and other bills to cover salaries. In Florida, a cancer center is racing to find money for chemotherapy drugs to avoid delaying critical treatments for its patients. And in Pennsylvania, a primary care doctor is slashing expenses and pooling all of her cash — including her personal bank stash — in the hopes of staying afloat for the next two months."[1] This is reality for many healthcare providers as a result of Change's response following what might be the most consequential data breach in history.

[1] Reed Abelson & Julie Creswell, *Cyberattack Paralyzes the Largest U.S. Healthcare Payment System*, NYTIMES (Mar. 7, 2024), https://www.nytimes.com/2024/03/05/health/cyberattack-healthcare-cash.html.

2. A ransomware group claims to have accessed Change's servers and seized 6 terabytes of critical confidential and highly sensitive information, resulting in network outages that have already impacted millions of patients and physicians across the country.[2] On February 21, 2024, Change disclosed that it was the subject of this massive data breach whereby hackers known as "ALPHV/Blackcat" ("Blackcat") gained unauthorized access to its networks (the "Data Breach").

3. Blackcat is a notable cybergroup that infiltrates healthcare institutions' internal servers through vulnerabilities in their networks. The group uses "ransomware to identify and attack 'high-value victim institutions[.]'"[3] According to the Department of Justice, Blackcat typically steals victims' data and encrypts the institution's data, networks, and servers, blocking the institution from accessing them. The group then demands the institution pay a ransom in exchange for the keys to decrypt the institution's network and servers. In exchange for ransom, Blackcat also offers a promise that it will not publish the institution's data to Blackcat's site on the Dark Web. Still, even when ransoms are paid, this data often ends up on the Dark Web. Blackcat has emerged as the second most prolific ransomware-as-a-service variant in the world.[4]

4. Blackcat accessed, copied, and exfiltrated highly sensitive information stored on Change's servers for millions of individuals, including active US military/navy personnel

[2] Steve Adler, *UnitedHealth Group Confirms Data Stolen in Change Healthcare Ransomware Attack*, THE HIPAA JOURNAL (Mar. 29, 2024), https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack.
[3] James Farrell, *Change Healthcare Blames 'Blackcat' Group for Cyber Attack That Disrupted Pharmacies and Health Systems*, FORBES (Feb. 29, 2024, 1:18 PM), https://www.forbes.com/sites/jamesfarrell/2024/02/29/change-healthcare-blames-blackcat-group-for-cyber-attack-that-disrupted-pharmacies-and-health-systems/?sh=589769fc1c4d.
[4] *Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant*, DOJ (Dec. 19, 2023), https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant.

identifiable information, medical records, dental records, payment information, claims information, patients' information (such as phone numbers, addresses, Social Security numbers, emails, etc.), insurance records, and more ("PHI").[5] Blackcat also encrypted portions of Change's network, rendering them unusable.

5. Blackcat has also shared the stolen data with other criminal affiliates.

6. Defendant reportedly paid a ransom of $22 million to Blackcat, but one of Blackcat's affiliates claims to still have a copy of the stolen data and that it was not paid its share of the ransom.[6]

7. The fallout from this Data Breach has and will wreak havoc on the healthcare industry. As a subsidiary of one of the largest healthcare insurers, Change processes 15 billion transactions annually, "touching one in three U.S. patient records."[7] But to stop the cybersecurity wound from bleeding further, Change decided to take certain systems offline. One of these systems is the Change Healthcare platform ("Change Platform"). This platform provides, among other things, a revenue and payment cycle management service that connects payers, providers, and patients within the U.S. healthcare system.[8] The Change Platform is widely used among practitioners.

---

[5] *MMRG Notifies Patients of Cybersecurity Incident*, BUSINESS WIRE (Feb. 6, 2024, 5:30 PM), https://www.businesswire.com/news/home/20240206060527/en/.

[6] Steve Adler, *UnitedHealth Group Confirms Data Stolen in Change Healthcare Ransomware Attack*, THE HIPAA JOURNAL (Mar. 29, 2024), https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack.

[7] Nicole Sganga & Andres Triay, *Cyberattack on UnitedHealth still impacting prescription access: "These are threats to life,"* CBS NEWS (Feb. 29, 2024, 9:00 PM), https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-prescription-access-still-impacted/.

[8] *Revenue Cycle Management*, CHANGE HEALTHCARE, https://www.changehealthcare.com/revenue-cycle-management (last visited Mar. 7, 2024).

8. Without the Change Platform, the healthcare industry is immobilized. Patients are stuck in prescription purgatory without access to their vital medications. This is especially disruptive to elderly patients who have a fixed income and cannot afford medications without insurance, as well as individuals with chronic illnesses who face life-threatening symptoms without their medication. Change's network outage is jeopardizing the health of millions of Americans.

9. Patients are not the only victims of the Data Breach. The ripple effect of the Data Breach is also hampering healthcare providers' practices. According to John Riggi, national advisor for cybersecurity and risk at the American Hospital Association, "… [T]his cyberattack has affected every hospital in the country one way or another."[9] Many providers are having trouble verifying patient eligibility and coverage, filing claims, and billing patients.[10] This leaves small and mid-sized practices especially vulnerable without normal cash flow to sustain operations. For the past two weeks, these healthcare practices have received little, if any, reimbursement from insurers for patient visits. Without these reimbursements, small and mid-sized practices cannot afford employee payroll, rent/mortgage, and medical supplies. The combination of unmedicated patients and handicapped healthcare providers paints a bleak future.

10. Exacerbating this crisis, Change has not provided adequate guidance to healthcare providers. Healthcare providers must notify their patients that their PHI may have been compromised by the Data Breach. And, under certain conditions, they must report this breach to

[9] Nicole Sganga & Andres Triay, *Cyberattack on UnitedHealth still impacting prescription access: "These are threats to life,"* CBS NEWS (Feb. 29, 2024, 9:00 PM), https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-prescription-access-still-impacted/.

[10] Associated Press, *Minnetonka Based United Healthcare Hacked*, KNSI (Feb. 29, 2024, 5:46 PM), https://knsiradio.com/2024/02/29/minnetonka-based-united-healthcare-hacked/.

the federal government. However, Change has not provided adequate accounts about the Data Breach that would allow healthcare providers to satisfy their obligations. Without Change's guidance, healthcare providers are in a state of uncertainty.

11. Born of Change's negligence, healthcare providers alike will feel the immediate effects of the network outage for some time. UnitedHealth Group Incorporated's ("UHG") Chief Operating Officer Dirk McMahon suggests that the outage could last weeks.[11] This delay would certainly put many healthcare practices out of business. To avoid this looming result, healthcare providers are incurring extra costs and switching to different healthcare software companies to assist with revenue and payment management. Once again, this hurts small and mid-sized practices the most. Not only are these practices weeks behind on receiving payment, but they must now pay for another service with their remaining funds and learn an entirely new system all the while continuing to treat patients.

12. Despite the disruption in its services and its failure to connect with healthcare providers, Change still manages to collect payment from healthcare practices.

13. Change is responsible for the Data Breach because it failed to implement reasonable security procedures and practices and failed to disclose material facts surrounding its deficient security protocols. Responding to the Data Breach, Change claims to have chosen to take systems offline to stop hackers from seizing more data than the 6 terabytes already taken. Change's decision caused this network outage that has severely impacted not only patients but healthcare practices and providers who rely on the Change Platform for processing claims and payment. As a result of Change's actions, Plaintiff and Class members did not receive the benefit of their bargain with

[11] Brittany Trang, *Change Healthcare cyberattack outage could persist for weeks, UnitedHealth Group executive suggests*, STAT (Feb. 29, 2024), https://www.statnews.com/2024/02/29/change-healthcare-cyber-attack-outage-will-last-for-weeks/.

Change and are not receiving the services that they have paid for. Furthermore, Plaintiff and Class members have not received payments for their healthcare services and have incurred extra costs from switching to another healthcare payment software.

## PARTIES

14. Plaintiff Paula S. Gordy LISW, LLC is an Iowa limited liability company with its principal place of business in Centerville, Iowa.

15. Defendant Change Healthcare Inc. is a Delaware corporation with its principal place of business in Nashville, Tennessee.

## JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members and at least some members of the proposed Class have a different citizenship from Change. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

17. This Court has jurisdiction over Change because it maintains and operates its headquarters in this District and/or is authorized to and does conduct business in this District.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) (1) & (2) because Change resides in this District and/or a substantial part of the events and omissions giving rise to this action occurred in this District.

## FACTUAL ALLEGATIONS

### *Change's Privacy Practices*

19. Change Healthcare is a healthcare technology company that provides data-driven and analytics-driven solutions for clinical, financial, administrative, and patient management to

healthcare providers.[12] It holds itself out as providing "data and analytics, plus patient engagement and collaboration tools" to "providers and payers [to] optimize workflows, access the right information at the right time, and support the safest and most clinically appropriate care."[13] Change is one of the largest processors of prescription medications in the United States and handles billing for more than 67,000 pharmacies across the country through which it handles 15 billion healthcare transactions annually.[14]

20. In the regular course of business, Change stores patients' highly sensitive health information collected from myriad clients like Medicare, pharmacies, healthcare providers, and so on. This includes patients' full names, phone numbers, addresses, Social Security numbers, emails, medical records, dental records, payment information, claims information, insurance records, and much more.

21. Given the amount and sensitive nature of the data it stores, Change maintains a privacy policy describing how confidential and personal information is used and disclosed: "[w]e implement and maintain organizational, technical, and administrative security measures designed to safeguard the data we process against unauthorized access, destruction, loss, alteration, or misuse. These measures are aimed at providing on-going integrity and confidentiality of data, including your personal information."

---

[12] OptumInsight and Change Healthcare Combine to Advance a More Modern, Information and Technology-Enabled Health Care Platform, OPTUM (Jan. 6, 2021), https://www.optum.com/en/about-us/news/page.hub.optuminsight-change-healthcare-combine.html.

[13] *The Change Healthcare Platform*, CHANGE HEALTHCARE, https://www.changehealthcare.com/platform (last visited Mar. 1, 2024).

[14] Zack Whittaker, *UnitedHealth confirms ransomware gang behind Change Healthcare hack amid ongoing pharmacy outages*, TECHCRUNCH (Feb. 29, 2024, 9:15 AM) https://techcrunch.com/2024/02/29/unitedhealth-change-healthcare-ransomware-alphv-blackcat-pharmacy-outages/.

22. Given its representations and experience handling highly sensitive PHI, Change understood the need to protect patients' PHI and prioritize data security.

***The Data Breach***

23. On February 21, 2024, in an SEC filing, UHG announced that "a suspected nation-state associated cyber security thread actor had gained access to some of the Change Healthcare information technology systems."[15] After detecting the breach, UHG claimed to have "proactively isolated the impacted systems from other connecting systems…"[16] UHG also said it was "working with law enforcement" and allegedly "notified customers, clients and certain government agencies" of the breach.[17] UHG disclosed that the "network interruption [was] specific to Change Healthcare…"[18]

24. Blackcat disclosed that the exfiltrated data includes millions of: "active US military/navy personnel PII," "medical records," "dental records," "payments information," "Claims information," "Patients PII including Phone numbers/addresses/SSN/emails/etc…," "3000+ source code files for Change Health solutions…," "Insurance records," and "many many more." Blackcat warned UHG that "you are walking on a very thin line be careful you just might fall over."

25. The Change Platform was disconnected following the Data Breach. Through the Change Platform, healthcare providers—who have paid for this service—submit insurance claims. These claims are sent to health insurance companies to evaluate and process. Providers then receive reimbursement payments from the insurance company.

---

[15] *UnitedHealth Group Incorporation Form 8-K*, SEC (Feb. 21, 2024), https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm.
[16] *Id.*
[17] Id.
[18] *Id.*

26. The Change Platform has been inoperable from the time of the breach through the filing of this Complaint and is projected to remain inoperable through at least mid-March.[19]

27. The Change Platform handles 15 billion healthcare transactions (or about one-in-three U.S. patient records). That means that the normal method of transmitting claims for payment has been disrupted for a huge swath of providers' claims. Moreover, many providers *only* use Change for claims submission, meaning that for those providers, the impact is has been to completely stop the flow of payments.

28. The potential impact of the Data Breach is enormous, and its effects are currently being felt by healthcare providers nationwide.

***The Data Breach was Preventable***

29. Change's cybersecurity practices and policies were inadequate and fell short of the industry-standard measures that should have been implemented long before the Data Breach occurred. This is especially true given that the healthcare industry is frequently one of the most targeted sectors for cyberattacks. Attacks using stolen credentials have increased precipitously over the last several years.

30. Healthcare providers and their affiliates like Change are prime targets because of the information they collect and store, including financial information of patients, login credentials, insurance information, medical records and diagnoses, and personal information of employees and patients—all extremely valuable on underground markets.

[19] https://www.unitedhealthgroup.com/changehealthcarecyberresponse (last visited March 13, 2024)

31. This was known and obvious to Change as it observed frequent public announcements of data breaches affecting healthcare providers and knew that information of the type it collected, maintained, and stored is highly coveted and a frequent target of hackers.

32. It is well known that use of stolen credentials has long been the most popular and effective method of gaining authorized access to a company's internal networks and that companies should activate defenses to prevent such attacks.

33. According to the Federal Bureau of Investigation (FBI), phishing schemes designed to induce individuals to reveal personal information, such as network passwords, were the most common type of cybercrime in 2020, with such incidents nearly doubling in frequency between 2019 and 2020.[20] According to Verizon's 2021 Data Breach Investigations Report, 43% of breaches stemmed from phishing and/or pretexting schemes.[21]

34. The risk is so prevalent for healthcare providers that on October 28, 2020, the FBI and two federal agencies issued a "Joint Cybersecurity Advisory" warning that they have "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[22] The Cybersecurity and Infrastructure Security Agency (CISA), the Department of Health and Human Services (HHS), and the FBI issued the advisory to warn healthcare providers to take "timely and reasonable precautions to protect their networks from these threats."[23]

---

[20] *2020 Internet Crime Report*, FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited Mar. 1, 2024).
[21] *2021 DBIR Master's Guide*, VERIZON, https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (subscription required) (last visited Mar. 1, 2024).
[22] *Ransomware Activity Targeting the Healthcare and Public Health Sector*, JOINT CYBERSECURITY ADVISORY, https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf (last visited Mar. 1, 2024).
[23] *Id*.

35. There are two primary ways to mitigate the risk of stolen credentials: user education and technical security barriers. User education is the process of making employees or other users of a network aware of common disclosure schemes and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients.

36. Through technical security barriers, companies can also greatly reduce the flow of fraudulent e-mails by installing software that scans all incoming messages for harmful attachments or malicious content and implementing certain security measures governing e-mail transmissions, including Sender Policy Framework (SPF) (e-mail authentication method used to prevent spammers from sending messages on behalf of a company's domain), DomainKeys Identified Mail (DKIM) (e-mail authentication method used to ensure messages are not altered in transit between the sending and recipient servers), and Domain-based Message Authentication, Reporting and Conformance (DMARC), which "builds on the widely deployed [SPF] and [DKIM] protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email."[24]

37. In addition to mitigating the risk of stolen credentials, the CISA guidance encourages organizations to prevent unauthorized access by:

- Conducting regular vulnerability scanning to identify and address vulnerabilities, particularly on internet-facing devices;
- Regularly patching and updating software to latest available versions, prioritizing timely patching of internet-facing servers and software processing internet data;
- Ensuring devices are properly configured and that security features are enabled;

[24] *Id.*

- Employing best practices for use of Remote Desktop Protocol (RDP) as threat actors often gain initial access to a network through exposed and poorly secured remote services; and
- Disabling operating system network file sharing protocol known as Server Message Block (SMB) which is used by threat actors to travel through a network to spread malware or access sensitive data.[25]

38. The CISA guidance further recommends use of a centrally managed antivirus software utilizing automatic updates that will protect all devices connected to a network (as opposed to requiring separate software on each individual device), as well as implementing a real-time intrusion detection system that will detect potentially malicious network activity that occurs prior to ransomware deployment.[26] Likewise, the principle of least privilege (POLP) to all systems should be applied to all systems so that users only have the access they need to perform their jobs.[27]

39. Despite holding the PHI of millions of patients, Change failed to adhere these recommended best practices. Indeed, had Change implemented common sense security measures like network segmentation and POLP, the hackers never could have accessed millions of patient files and the breach would have been prevented or much smaller in scope. Change also lacked the necessary safeguards to detect and prevent phishing attacks and failed to implement adequate monitoring or control systems to detect the unauthorized infiltration after it occurred.

[25] Multi-State Information Sharing & Analysis Center, Ransomware Guide 4, CISA.GOV (Sept. 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf.
[26] *Id.* at 5.
[27] *Id*. at 6.

40. Change, like any entity in the healthcare industry its size storing valuable data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to millions of patient files. Change's below-industry-standard procedures and policies are inexcusable given its knowledge that it was a prime target for cyberattacks.

***The Aftermath of the Data Breach***

41. As a result of the Data Breach, Change disconnected certain systems including its Change Platform used by healthcare providers nationwide in connection with payment and treatment. Change did this without an adequate substitute. This decision is decimating healthcare practices nationwide.

42. Because Change disconnected the Change Platform, many healthcare providers have lost their primary (and in some cases their *only*) source of processing payments for their services through patients' healthcare plans and thus are not receiving payment. Healthcare providers are absorbing these upfront costs.

43. A dwindling account balance coupled with outstanding reimbursement has put many healthcare providers in a precarious position. For instance, Arlington Urgent Care, a chain of five urgent care centers around Columbus, Ohio, has about $650,000 in unpaid insurance reimbursements. The owners have taken lines of credit from banks and used their personal saving to afford employee payroll, rent, and other expenses.[28] Other healthcare providers are racking up duplicated payment software charges. Florida Cancer Specialists and Research Institute in Gainesville switched to two other healthcare software platforms because "it spends $300 million

[28] Reed Abelson & Julie Creswell, *Cyberattack Paralyzes the Largest U.S. Healthcare Payment System*, NYTIMES (Mar. 7, 2024), https://www.nytimes.com/2024/03/05/health/cyberattack-healthcare-cash.html.

a month on chemotherapy and other drugs for patients whose treatments cannot be delayed."[29] And some healthcare providers are cutting resources for patients to persevere through this. A Philadelphia-based primary care practice with 20 clinicians has mailed off "hundreds and hundreds" of pages Medicare claims and is contemplating cutting expenses by "reducing the supply of vaccines the clinic has on hand."[30]

44. Healthcare providers are not receiving Change's services that they paid for, and without these services, these providers and practices are struggling to care for patients and are losing money. As such, Plaintiff and Class members did not receive the benefit of their bargain with Change because they paid for the value of services they did not receive.

45. Moreover, scammers have begun targeting patients affected by the Data Breach. The scammers are pretending to represent medical providers to demand payment for services, leading to increased calls to providers and additional time spent by those providers to respond to patient inquiries.[31]

***Allegations Relating to Plaintiff Paula S. Gordy LISW, LLC***

46. Plaintiff Paula S. Gordy LISW, LLC, is an Iowa limited liability company based in Centerville, Iowa.

47. Plaintiff contracted with Change Healthcare for its platform that provides revenue and payment cycle management services.

48. Plaintiff, through its owner Paula S. Gordy, provides counseling services to its patients and relies on the Change Healthcare system to submit claims and receive payments.

[29] *Id*.
[30] *Id*.
[31] *See supra* note 6.

49. Through the Change Platform, Plaintiff submits insurance claims. The claims are sent to insurance companies for evaluation and processing. Once the claims are approved, Plaintiff receives payment.

50. As a result of the data breach, Plaintiff has faced significant cash flow disruptions due to an inability to submit claims or receive payments.

51. Because of the Data Breach, Plaintiff has had to spend additional time and considerable expense to find and secure another platform to complete Plaintiff's billing requirements.

52. Because of the Data Breach, Plaintiff has had to cancel appointments and turn away further business so that any available time could be spent responding to the Data Breach, paying employees, and collected monies owed.

53. The added time and expense Plaintiff has been forced to incur has placed, and continues to place, significant strain on Plaintiff's finances and threatens the future viability of Plaintiff's practice.

***Change Failed to Comply with Federal Law and Regulatory Guidance***

54. Change is covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (see 45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

55. These rules establish national standards for the protection of patient information, including PHI, defined as "individually identifiable health information" which either "identifies

the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. 45 C.F.R. § 160.103.

56. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."[32]

57. HIPAA requires that Change implement appropriate safeguards for this information.[33]

58. HIPAA requires that Change provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—i.e. non-encrypted data.[34]

59. Despite these requirements, Change failed to comply with its duties under HIPAA and its own privacy policies. Indeed, Change failed to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Adequately protect the PHI of patients;

c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

[32] 45 C.F.R. § 164.502.
[33] 45 C.F.R. § 164.530(c)(1).
[34] 45 C.F.R. § 164.404; 45 C.F.R. § 164.402.

e. Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

60. Additionally, federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[35]

[35] *Start with Security*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Mar. 1, 2024).

61. The FTC's publication *Protecting Personal Information: A Guide for Business* sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.[36] Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[37]

62. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security; monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[38] This is consistent with guidance provided by the FBI, HHS, and the principles set forth in the CISA 2020 guidance.

63. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders

[36] *Protecting Personal Information*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Mar. 1, 2024).
[37] *Id*.
[38] Start With Security, supra note 41.

resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[39]

64. Change was fully aware of its obligation to implement and use reasonable measures to protect the PHI of the patients but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. Change's failure to employ reasonable measures to protect against unauthorized access to patient information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

## CLASS ACTION ALLEGATIONS

65. Plaintiff seeks relief in its individual capacity and as a representative of all others who are similarly situated. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff brings this action on behalf of itself and the Class defined as: All healthcare providers whose reimbursement payments were delayed following the Data Breach announced by UnitedHealth Group Incorporated in February 2024 (the "Class").

66. Specifically excluded from the Class are Defendant; its officers, directors, or employees; any entity in which Defendant has a controlling interest; and any affiliate, legal representative, heir, or assign of Defendant.

67. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

[39] *Privacy and Security Enforcement*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Mar. 1, 2024).

68. Class Identity: The members of the Class are readily identifiable and ascertainable. Change and/or its affiliates, among others, possess the information to identify and contact class members.

69. Numerosity: The members of the Class are so numerous that joinder of all of them is impracticable. According to the U.S. Department of Health and Human Services, Change "processes 15 billion health care transactions annually and is involved in one in every three patient records." According to Change, it is connected to "more than 600,000 providers[.]"

70. Typicality: Plaintiff's claims are typical of the claims of the members of the Class because all class members reimbursement payments were delayed following the Data Breach and were harmed as a result.

71. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has no known interest antagonistic to those of the Class and its interests are aligned with Class members' interests. Plaintiff's reimbursement payments were delayed following the Data Breach just as class members and suffered similar harms. Plaintiff has also retained competent counsel with significant experience litigating complex and commercial class actions.

72. Commonality and Predominance: There are questions of law and fact common to the Class such that there is a well-defined community of interest in this litigation. These common questions predominate over any questions affecting only individual class members. The common questions of law and fact include, without limitation:

- Whether Change owed Plaintiff and class members a duty to implement and maintain reasonable security procedures and practices to protect patients' PHI;
- Whether Change received a benefit without proper restitution making it unjust for Change to retain the benefit without commensurate compensation;

- Whether Change acted negligently in connection with the monitoring and/or protection of Plaintiff's and class members' PHI;
- Whether Change violated its duty to implement reasonable security systems to protect Plaintiff's and class members' PHI;
- Whether Change's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiff and class members;
- Whether Change adequately addressed and fixed the vulnerabilities that enabled the Data Breach;
- Whether Change breached agreements with Plaintiffs and Class members by disconnecting the Change Platform; and
- Whether class members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

73. Change has engaged in a common course of conduct and Plaintiff and class members have been similarly impacted by Change's failure to maintain reasonable security procedures and practices to protect patients' PHI.

74. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all class members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiff

knows of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules.

## CLAIMS FOR RELIEF

### COUNT I
**Negligence**
***(On Behalf of Plaintiffs and the Class)***

75. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

76. Change required patients' PHI as a condition of receiving healthcare services and to perform Change's functions in connection with patients receiving medical treatment. Change stored the data for purposes of providing health insurance services as well as for commercial gain.

77. Change owed Plaintiff and class members a duty to exercise reasonable care in protecting their PHI from unauthorized disclosure or access. Change acknowledged this duty in its privacy policies, where it promised not to disclose PHI, including SSNs, without authorization and to abide by all federal laws and regulations.

78. Change owed a duty of care to Plaintiff and class members to provide adequate data security, consistent with industry standards, to ensure that Change's systems and networks adequately protected the PHI.

79. Defendant's duty to use reasonable care in protecting PHI arises as a result of the parties' relationship, as well as common law and federal law, including the HIPAA regulations described above and Change's own policies and promises regarding privacy and data security.

80. Change knew, or should have known, of the risks inherent in collecting and storing PHI in a centralized location, Change's vulnerability to network attacks, and the importance of adequate security.

81. Change breached its duty to Plaintiff and class members in numerous ways, as described herein, including by:

- Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect patients' PHI;
- Failing to comply with industry standard data security measures for the healthcare industry leading up to the Data Breach;
- Failing to comply with its own privacy policies;
- Failing to comply with regulations protecting the PHI at issue during the period of the Data Breach; and
- Failing to adequately monitor, evaluate, and ensure the security of Change's network and systems;

82. Patients' PHI would not have been compromised but for Change's wrongful and negligent breach of its duties.

83. Change would not have disconnected the Change Platform but for its wrongful and negligent breach of its duties.

84. Change's failure to take proper security measures to protect patients' as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and copying of PHI by unauthorized third parties. Given that healthcare providers and affiliates are prime targets for hackers, patients are part of a foreseeable, discernible group that was at high risk of having their PHI misused or disclosed if not adequately protected by Change. It was also foreseeable that as a result of a data breach, Change would have to disconnect systems that could disrupt its customers' healthcare practices.

85. As a direct and proximate result of Change's conduct, Plaintiff and class members have suffered damages, including missed payments and out-of-pocket expenses associated with (i) purchasing new healthcare payment software; (ii) notifying patients of data breach; and (iii) late

penalties assessed for untimely payment of expenses. Furthermore, Plaintiff and class members' damages include time and effort spent researching and implementing new healthcare payment software.

**COUNT II**
**Breach of Contract**
***(On Behalf of Plaintiffs and the Class)***

86. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

87. Acting in the ordinary course of business, Change contracts with healthcare providers, like Plaintiff and Class members, to provide its Change Platform. This platform allows Change to, among other things, act as a middleman between healthcare providers and insurance companies. Healthcare providers submit insurance claims through the Change Platform, which Change sends to the insurance companies. After evaluation and processing, insurance companies then pay the healthcare providers.

88. Plaintiff and Class members paid for Change's Platform.

89. In return for their payment, Plaintiff and Class members were promised access and use of the Change Platform.

90. In February 2024, following the Data Breach, Change disconnected the Change Platform thereby severing Plaintiff's and Class members' access and use of the Change Platform and breaching its contractual obligations.

91. As a direct and proximate result of Change's breaches, Plaintiff and class members sustained actual losses and damages. Plaintiff and class members alternatively seek an award of nominal damages.

## COUNT III
**Unjust Enrichment**
***(On Behalf of Plaintiffs and the Class)***

92. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

93. Plaintiff and class members have an interest, both equitable and legal, in their injuries that arose from Change's wrongful conduct.

94. Plaintiff and Class members conferred a benefit on Change in the form of monetary payment.

95. Change appreciated and had knowledge of the benefits conferred upon it by Plaintiff and Class members.

96. In exchange for receiving Plaintiff's and Class members' money, which provided Change commercial gain, Change should have supplied Plaintiff and Class members' with uninterrupted access and use of its Change Platform. However, Change disconnected the Change Platform following the Data Breach.

97. As a result of Change's conduct, Plaintiff and Class members suffered actual damages as described herein. Under principles of equity and good conscience, Change should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds they received from Plaintiff and Class members.

## COUNT IV
**Declaratory Judgment**
***(On Behalf of Plaintiffs and the Class)***

98. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

99. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant

further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

100. An actual controversy has arisen in the wake of the Data Breach regarding Change's present and prospective common law and other duties to reasonably safeguard PHI and whether Change is currently maintaining data security measures adequate to protect patients from further cyberattacks and data breaches that could compromise their PHI and therefore prevent healthcare providers from remaining without use of the Change Platform, which is a lynchpin of their payment practices.

101. Change still possesses PHI pertaining to Plaintiff and class members, which means their PHI remains at risk of further breaches because Change's data security measures remain inadequate. Another data breach would likely result in Change disconnecting the Change Platform again causing further injuries to Plaintiff and Class members.

102. Pursuant to the Declaratory Judgment Act, Plaintiff seeks a declaration that: (a) Change's existing data security measures do not comply with its obligations and duties of care; and (b) in order to comply with their obligations and duties of care, (1) Change must have policies and procedures in place to ensure the parties with whom it shares sensitive personal information maintain reasonable, industry-standard security measures, including, but not limited to, those listed at (ii), (a)-(i), infra, and must comply with those policies and procedures; (2) Change must: (i) purge, delete, or destroy in a reasonably secure manner patients' PHI if it is no longer necessary to perform essential business functions so that it is not subject to further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

- Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on

Change's systems on a periodic basis, and ordering Change to promptly correct any problems or issues detected by such third-party security auditors;

- Engaging third-party security auditors and internal personnel to run automated security monitoring;
- Auditing, testing, and training its security personnel regarding any new or modified procedures;
- Encrypting PHI and segmenting PHI by, among other things, creating firewalls and access controls so that if one area of Change's systems is compromised, hackers cannot gain access to other portions of its systems;
- Purging, deleting, and destroying in a reasonable and secure manner PHI not necessary to perform essential business functions;
- Conducting regular database scanning and security checks;
- Conducting regular employee education regarding best security practices;
- Implementing multi-factor authentication and POLP to combat system-wide cyberattacks; and
- Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

**REQUEST FOR RELIEF**

103. WHEREFORE, Plaintiff, on behalf of himself and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiff as class representatives and Plaintiff's counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit and prevent Change from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and class members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court award statutory damages, trebled, and/or punitive or exemplary damages, to the extent permitted by law;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Change as a result of their unlawful acts, omissions, and practices;

F. That Plaintiff be granted the declaratory and injunctive relief sought herein;

G. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

H. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs hereby demand a jury trial in the instant action.

Dated: April 4, 2024

*/s/ J. Gerard Stranch, IV*

J. Gerard Stranch, IV (BPR #23045)
Grayson Wells (BPR #039658)
Michael Iadevaia, BPR 041622
Emily Schiller, BPR 039387
**STRANCH, JENNINGS & GARVEY, PLLC**
223 Rosa L. Parks Ave., Ste 200
Nashville, TN 37203
Phone: 615-254-8801
Fax: 615-255-5419
gstranch@stranchlaw.com
gwells@stranchlaw.com
miadevaia@stranchlaw.com
eschiller@stranchlaw.com

Gary M. Klinger*
Patrick Montoya*
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLC**
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
gklinger@milberg.com
pmontoya@milberg.com

Jeff Ostrow*
Ken Grunfeld*
Jonathan M. Streisfeld*
**KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT**
One West Las Olas Blvd, Suite 500
Fort Lauderdale, FL 33301
Phone: 954.525.4100
ostrow@kolawyers.com
streisfeld@kolawyers.com

**Pro Hac Vice Forthcoming*

*Counsel for Plaintiff and the Class*